PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/10

A1

(11) International Publication Number: WO 00/26868

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/EP99/08258

(22) International Filing Date: 27 October 1999 (27.10.99)

(30) Priority Data:
198 50 293.1 30 October 1998 (30.10.98) DE

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: THÜRINGER, Peter [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL). RIEGER, Edgar [AT/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Agent: SCHMALZ, Günther; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

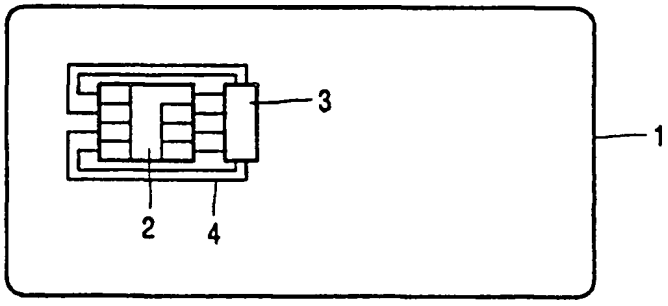
(81) Designated States: CN, JP, KR, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: DATA CARRIER WITH PROTECTION AGAINST SPY OUT

(57) Abstract

In a data carrier with a data processing device in which there is provided an external as well as an internal power supply, it is proposed to provide at least one switching means which is accommodated in the data carrier in order to realize temporary decoupling of the external power supply, thus making the retrieval of sensitive data impossible.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Data carrier with protection against spy out.

The invention relates to a data carrier with a data processing device as well as to an electronic component with a data processing device for such a data carrier.

Recently doubts have arisen as regards the security of data carriers, it being claimed that security-relevant data can be discovered by observation of the power consumption of such a data carrier.

It is an object of the invention to ensure that such attempts cannot be successful.

This object is achieved according to the invention in that a data carrier with an external power supply is also provided with an internal power supply, at least one switching means being provided in the data carrier in order to realize temporary decoupling of the external power supply.

The advantage of the invention resides in the fact that the decoupling of the external power supply, preferably during security-relevant operations or at least partly during security-relevant operations of the data processing device, frustrates such attempts to fraud.

Advantageous embodiments of the invention are described in the dependent Claims.

The invention will be described in detail hereinafter.

Data carriers provided with data processing devices, for example so-called chip cards, incorporate a test function for the protection of security-relevant transactions, for example the dispensing of cash in money-dispensing machines; such a test function serves to test the authorization for the transaction. In order to establish proof of authorization, use is made of, for example so-called Personal Identification Numbers (PIN). The PIN can be tested in the data processing device of the data carrier while utilizing key algorithms. The power supply for the data carrier is customarily realized by way of contacts or by induction of alternating currents which are converted into a direct current in the data carrier.

Fig. 1 shows a so called chip card 1 with a contact field 2 and an embedded chip 3. The chip 3 is connected to the contact field 2 via internal wires 4.

In order to preclude with certainty, at least during the testing of the transaction authorization, the retrieval of information regarding the authorization key via the externally applied and hence measurable current consumption, or via the signals applied via the current leads, the supply leads to the external current source are decoupled by means of decoupling means, for example switches. In this manner it is prevented that signals which are produced by internal operations can reach the environment. An internal power supply source is used for the power supply of the data processing device at least for this period of time. Suitable for this purpose are, for example, rechargeable batteries, a solar cell, illuminated by a read apparatus, or capacitors which are proportioned so that the power supply is ensured at least during the decoupling time. Power supply beyond that time is not required so as to ensure the intended decoupling step. The duration of the decoupling for the purpose of disguising the operating time can be controlled not only by the data processing device itself but also, for example in a time-controlled manner or until the energy of the internal power supply source has decreased to a given value.

Fig. 2 shows the internal structure of a preferred embodiment of a chip 3. Inside the chip there is provided the data processing section 5 in which the security-relevant operations are carried out. To this end the data processing section 5 is connected to the contact field 2, i.e. to the contacts used for transmitting data from and to the data processing section 5. The current supply contact V of the contact field 2 is connected to a first switch 6 which is used as said decoupling device. The other end of the first switch 6 is connected to the power supply input of the data processing section 5. Also connected to this power supply input of the data processing section 5 are a capacitor 7 which is used as said internal supply source and a second switch 8 which is used as a discharging device. The first and the second switch 6,8 are controlled by a power supply control circuit 9. Preferably, the data processing section 5, the first and the second switch 6,8, the capacitor 7 and the power supply control circuit are arranged on a single chip so as to make it harder to deactivate parts of that arrangement by opening the chip card 1.

When the internal power supply sources cannot be proportioned so as to enable complete execution of the security-relevant operations during a single decoupling period, the security-relevant operations are preferably subdivided into a number of sub-operations; the internal power supply should then be capable of providing the power supply for at least each sub-operation. The circuit elements fed by the internal power source are thus decoupled from the external power supply at least during such sub-operations.

For example, the decoupling is triggered by switching means which are preferably arranged in such a manner that only weak coupling capacitances occur between internal and external power supply leads.

Additionally, in order to cover any capacitively coupled small signals or small signals arising by irradiation, noise or masking or superposition signals can be applied via the leads connected to the external power supply.

When a capacitor is used as an internal power supply source, for example supporting and smoothing capacitors provided on the chip can be used. These capacitors are discharged during the sensitive internal operations or sub-operations and recharged between the sub-operations, or after the operation, via the external power supply. Preferably, prior to such recharging the internal power supply source is always adjusted to the same discharged state or to different charging states due to incidental power consumption. Thus, sensible information as regards the arithmetic operations performed during the decoupling phase cannot be derived either by measurement of the current required for the recharging.

CLAIMS:

1. A data carrier with a data processing device which is provided with an external as well as with an internal power supply, at least one switching means being provided in the data carrier in order to realize temporary decoupling of the external power supply.

2. A data carrier as claimed in Claim 1, characterized in that the decoupling of the external power supply takes place at least partly during predetermined states of operation of the data processing device.

3. A data carrier as claimed in Claim 1 or 2, characterized in that a (rechargeable) battery, a capacitor or a solar cell is provided as the internal power supply.

4. A data carrier as claimed in Claim 1, 2 or 3, characterized in that prior to the cancellation of the decoupling there is performed a discharging operation or a loading operation of the internal power supply source which is random controlled or takes place to a predetermined value.

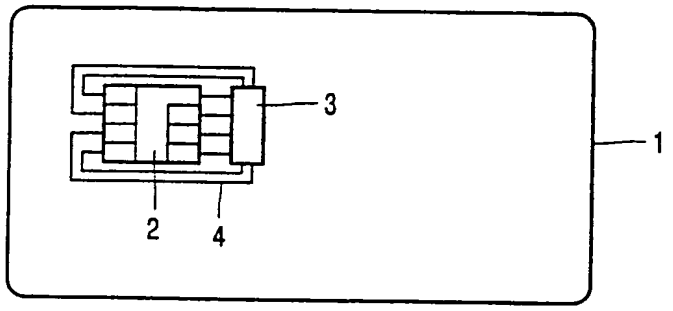


FIG. 1

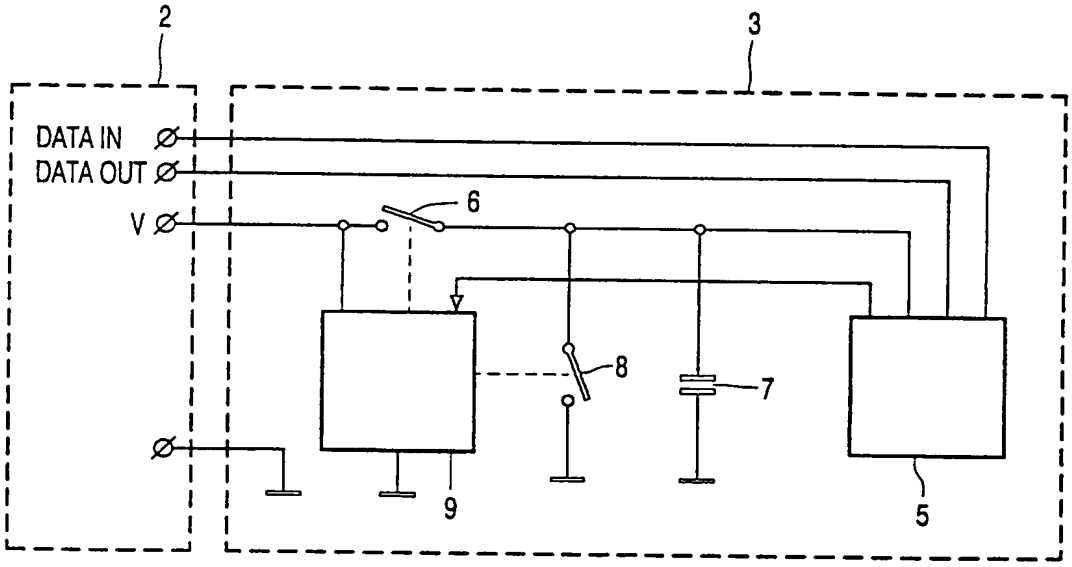


FIG. 2